Introduction to the HICSS-53 Minitrack on Innovative Behavioral IS Security and Privacy Research

Merrill Warkentin
Mississippi State University
m.warkentin@msstate.edu

Anthony Vance
Temple University
anthony@vance.name

Allen C. Johnston
University of Alabama
ajohnston@cba.ua.edu

This minitrack provides a venue for innovative research that rigorously addresses the risks to information system security and privacy, with a specific focus on individual behaviors within this nomological net. Domains include work related to detecting, mitigating, and preventing both internal and external human threats to organizational security. Papers may include theory development, empirical studies (both quantitative and qualitative), case studies, and other high-quality research manuscripts.

This year, the minitrack features nine papers addressing a range of behavioral security and privacy research questions that will stimulate further discussion and exploration of the key phenomena within this domain.

One group of papers addresses research issues related to addresses privacy research issues, including conflicts between privacy and security goals, information sharing in social networks, and the effect of textual priming on privacy concerns.

- Olt, Wagner. "Having Two Conflicting Goals in Mind: The Tension Between IS Security and Privacy when Avoiding Threats"
- El-Gayar, Mitchell. "The effect of privacy policies on information sharing behavior on social networks: A Systematic Literature Review"
- Buck, Dinev. "Low Effort and Privacy – How Textual Priming Affects Privacy Concerns of Email Service Users"

A second group of papers featured within this minitrack is focused on research topics related to end-user security behaviors, such as the role of financial incentives, post-data breach strategies, and information security role identity.

- Goel, Williams, Huang, Warkentin. "Understanding the Role of Incentives in Security Behavior"
- Ayaburi, Andoh-Baidoo, Lee. "Post Data Breach Use of Protective Technologies: An Examination of Users' Dilemma"
- Ogbanufe. "Information Security Is Not Really My Job": Exploring Information Security Role Identity in End-Users"

Finally, a third group also includes three papers on security in organizations. These involve the dark side of trust in cybersecurity, how abusive management gives rise to computer abuse, and dimensions of cybersecurity success.

- Pienta, Tams, Thatcher. "Can Trust be Trusted in Cybersecurity?"
- Nehme, George. "Taking It Out on IT: A Mechanistic Model of Abusive Supervision and Computer Abuse"
- Clark, Espinosa, DeLone. "Defending Organizational Assets: A Preliminary Framework for Cybersecurity Success and Knowledge Alignment"

We believe that this year's contributions will lead to interesting discussion and will advance our knowledge of information security within our discipline.

URI: https://hdl.handle.net/10125/64257
978-0-9981331-3-3
(CC BY-NC-ND 4.0)